BeaverTail, Software S1246 | MITRE ATT&CK®

Archived: 2026-04-05 16:32:28 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BeaverTail has used HTTP GET request to download malicious payloads to include InvisibleFerret and HTTP POST to exfiltrate data to C2 infrastructure.[5][1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

BeaverTail has collected and archived sensitive data in a zip file.[5]

Enterprise T1217 Browser Information Discovery

BeaverTail has searched the victim device for browser extensions including those commonly associated with cryptocurrency wallets.[2][6][5][7][3][1][8]

Enterprise T1059 .007 Command and Scripting Interpreter: JavaScript

BeaverTail has executed malicious JavaScript code.[2][6][3][4][1] BeaverTail has also been compiled with the Qt framework to execute in both Windows and macOS.[8]

Enterprise T1555 Credentials from Password Stores

BeaverTail has collected keys stored for Solana stored in `.config/solana/id.json` and other login details associated with macOS within `/Library/Keychains/login.keychain` or for Linux within `/.local/share/keyrings`.[3]

.001 Keychain

BeaverTail has collected keys associated with macOS within `/Library/Keychains/login.keychain`.[5][7][3]

.003 Credentials from Web Browsers

BeaverTail has stolen passwords saved in web browsers.[2][5][7][8] BeaverTail has also been known to collect login data from Firefox within key3.db, key4.db and logins.json from `/.mozilla/firefox/` for exfiltration.[3]

Enterprise T1005 Data from Local System

BeaverTail has exfiltrated data collected from local systems.[5][3][1][8]

Enterprise T1001 .001 Data Obfuscation: Junk Data

BeaverTail has added junk data or a dummy character prepended to a string to hamper decoding attempts.[3]

Enterprise T1074 .001 Data Staged: Local Data Staging

BeaverTail has staged collected data to the system’s temporary directory.[5]

Enterprise T1041 Exfiltration Over C2 Channel

BeaverTail has exfiltrated data collected from victim devices to C2 servers.[5][1][8]

Enterprise T1083 File and Directory Discovery

BeaverTail has searched for .ldb and .log files stored in browser extension directories for collection and exfiltration.[5][7][3]

Enterprise T1657 Financial Theft

BeaverTail has searched the victim device for browser extensions commonly associated with cryptocurrency wallets.[2][6][3][1][8]

Enterprise T1070 .004 Indicator Removal: File Deletion

BeaverTail has deleted files from a compromised host after they were exfiltrated.[5]

Enterprise T1105 Ingress Tool Transfer

BeaverTail has been used to download a malicious payload to include Python based malware InvisibleFerret.[2][5][7][3][1][8]

Enterprise T1654 Log Enumeration

BeaverTail has identified .ldb and .log files stored in browser extension directories for collection and exfiltration.[3]

Enterprise T1036 Masquerading

BeaverTail has masqueraded as MiroTalk installation packages: "MiroTalk.dmg" for macOS and "MiroTalk.msi" for Windows, and has included login GUIs with MiroTalk themes.[8]

Enterprise T1571 Non-Standard Port

BeaverTail has communicated with C2 IP addresses over ports 1224 or 1244.[3][1][8]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

BeaverTail has obfuscated strings of code with Base64 encoding within the JavaScript version of the malware.[3][1][8] BeaverTail has also utilized the open-source tool JavaScript-Obfuscator to obfuscate strings and functions.[2][4]

Enterprise T1195 .001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools

BeaverTail has been hosted on code repositories and disseminated to victims through NPM packages.[2][6][4][1][8]

Enterprise T1082 System Information Discovery

BeaverTail has been known to collect basic system information.[2][1] BeaverTail has also collected data to include hostname and current timestamp prior to uploading data to the API endpoint `/uploads` on the C2 server.[3]

Enterprise T1124 System Time Discovery

BeaverTail has obtained and sent the current timestamp associated with the victim device to C2.[3]

Enterprise T1204 .002 User Execution: Malicious File

BeaverTail has been executed through lures involving malicious JavaScript projects or trojanized remote conferencing software such as MicroTalk or FreeConference.[3][8] BeaverTail has also been executed through macOS and Windows installers disguised as chat applications.[2][4]
